ATAC TECHNICAL STANDARDS

developed by the

ATAC TECHNICAL STANDARDS WORKGROUP

Edited by A. Stewart Ferguson, Ph.D.

1.0 Participants

This document is the result of discussions held by the ATAC Technical Standards Workgroup during the period of September 1999 to February 2000. Participants included (in alphabetical order):

- William Applebee, *Consultant* (William@Applebee.net)
- Tom Bohn, *AFHCAN Project* (TBohn@AFHCAN.org)
- Terry Daniels, *Daniels, Tschannen & Associates* (warpspd@Alaska.net)
- Kathy Fanning, Veterans Administration (Kathy.Fanning@med.va.gov)
- Jeff Farnsworth, *U.S. Air Force*
- Stewart Ferguson, *AFHCAN Project* (Sferguson@AFHCAN.org)
- Steve Fletcher, *AT&T* (Sfletcher@Alascom.att.com)
- Doug LaMarche, *AT&T* (Dlamarche@Alascom.att.com)
- Greg Loudon, *SAIC* (loudong@saic.alaska.net)
- Capt. Steven Menzies, *U.S. Air Force* (steven.menzies@elmendorf.af.mil)
- Tom Nighswander, *ATAC* (TNighswander@ANTHC.org)
- Kelly Nokelby, *SAIC* (Nokelby@saic.alaska.net)
- Leigh Thurston, *Fairbanks Memorial Hospital* (LThursto@LHSnet.com)
- Marijo Toner, *Bartlett Regional Hospital* (mctoner@hisea.org)

2.0 Context

The Alaska Telehealth Advisory Commission (now the Alaska Telehealth Advisory Council) established four core guiding principles for the development of telehealth technologies throughout the state of Alaska. Outlined in the Final Report in 1999 [1], the second of these core principles states:

> *All entities participating in telehealth must assure that their systems meet inter-connectivity and interoperability standards and participate in the coordination of other telehealth efforts.*

Interoperability, as it being used within this report, is defined by the General Services Administration [2] as:

> *Interoperability 1. The ability of systems, units, or forces to provide services to and accept services from other systems, units or forces and to use the services so exchanged to enable them to operate effectively together.*
> *2. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases.*

Fifteen projects were identified in the ATAC Final Report, and it was suggested that an "open architecture" design would be in the best interest of the state to allow these systems to communicate with each other. An "open system" is defined as [2]:

> *A system with characteristics that comply with specified, publicly maintained, readily **available** standards and that therefore can be connected to other systems that comply with these same standards.*

Recognizing that an "open system" is defined in terms of publicly maintained standards, ATAC proposed to:

> *…implement a technical work group to assist in the development and facilitation of the interoperability of telehealth systems within the State.*

Subsequent to the ATAC Final Report issued on June 30, 1999, the ATAC Technical Standards Workgroup was formed and met eight times during the period of September 1999 to February 2000. The workgroup participants recognized that a set of standards is no assurance that systems will inter-operate, regardless of the rigor established and enforced by the standards. Many examples exist which demonstrate that standards by themselves cannot guarantee, but can promote, interoperability.

The workgroup also recognized that setting technical standards may provide significant benefits aside from promoting interoperability. Consequently, the workgroup opted to define a reasonable set of technical standards that should be met by all future telehealth applications, to:

- Enhance the interoperability of disparate telehealth systems and applications
- Improve the sustainability and usability of such systems in future years
- Provide a mechanism for meeting current and projected needs for data security

The first goal would meet those addressed by the ATAC Final Report. The second goal is independent of cooperation with other telehealth systems, but answers the question; "Will a system implemented today be usable in 20 years?" Will patient data recorded with one system be accessible when the software manufacturer no longer exists, or when a different system is implemented? The third goal was added because the workgroup felt the issue of security was sufficiently important and not necessarily covered by the first two goals.

The workgroup often reflected on the "power" of any standards to attain these goals. The objective was to set "reasonable" expectations on telehealth implementations that would not necessarily preclude specific solutions, but which would achieve the above specifications. Existing projects would only be expected to meet these standards if the projects expect to expand beyond their current implementation.

Generally speaking, the workgroup did not set any new standards, but embraced existing "industry" and "open standards" whenever possible. Standards that are specific to vendors or manufacturers are only permissible when no other alternatives exist, or when the manufacturer has established a *defacto* industry standard.

The Technical Standards Workgroup emphasizes that these technical standards are *recommendations* that, if followed, increase the likelihood of telemedicine systems reaching the above goals. The workgroup recommends that both vendors and customers alike follow these standards during the design, development and deployment of telemedicine systems.

Finally, the workgroup strongly believes the following statement:

> *Standards should be simple to be effective.*

3.0 Extent of Standards

Technical standards are inseparable from the state of current technology – as one changes, so must the other. Consequently, these standards are "snap shots" in time and may not necessarily be relevant as technology changes. For example, setting standards based on the XMLand HL7 file format may not be relevant in 10 years and certainly was not relevant 10 years ago when these technologies did not exist.

The following caveat applies to all technical standards established by the Technical workgroup and presented in this document:

- **3.0.1 The technical standards presented in this document reflect the "state of technology" at the current time, and must be reviewed and modified as technology changes. This document is a "living document"**

and must be maintained to adequately reflect these changes. It is reasonable to review these standards on an "as needed" basis for this purpose.

4.0 Security

The security of confidential patient health data is the legal, moral and ethical responsibility of all entities involved in telemedicine [3]. Security can be considered at several levels: protecting data from unauthorized access (encryption), verifying the source of data (authentication and nonrepudiation), and guaranteeing the integrity of data during transmission or storage (hash functions). The fundamental principle for security, established in the Federal Privacy Act of 1974 for federal systems [4], is that systems must "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

Standards exist at the Federal (and possibly state and local levels) concerning the storage and transmission of confidential patient health data. In some cases, the standards only apply to specific forms of data or specific forms of transmission.

HCFA (the Health Care Financing Administration, the federal agency that administers the Medicare/Medicaid/Child Health Insurance Programs, has adopted a policy that covers Internet transmission of HCFA Information [5]. The HCFA Internet Security Policy covers Internet data transmission only. It does not cover local data-at-rest (storage), or LAN transmission of data. It only applies to "HCFA Privacy Act-protected Data", not all electronic patient data. For example, Medicaid data not sent to HCFA is not covered by this policy. Nonetheless, this policy clearly defines that "a complete Internet communications implementation must include *adequate encryption*, employment of *authentication or identification* of communications partners, and a management scheme to incorporate *effective password/key management* systems." Moreover, the policy defines acceptable encryption algorithms as of November 1998, and outlines the possible procedures for implementing security: hardware-based encryption, software-based encryption, authentication, and identification. For example, the policy states that algorithms such as Triple 56 bit DES and Secure Sockets Layer (SSL) Version 3.0 are acceptable.

A more restrictive set of procedures is currently being proposed at the Federal level [6] to implement the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This policy is expected to become Federal law in 2000. It is much broader than the HCFA regulations, covering more types of data and many more aspects than merely Internet encryption and authentication. It delineates the individual security issues of access control, audit control, authorization control, data authentication and entity authentication. The policy details 55 mapped standards concerning security, including DES (ANSI X3.92 Data Encryption Standard) and triple DES (ANSI X9.52 Triple DES Modes of Operation) encryption algorithms.

As more sophisticated encryption techniques are becoming available and easier to implement, the trend is towards standards that effectively utilize these techniques for all data over all forms of transport. To ensure future compliance, proposed standards would adopt the "best" or "most restrictive" of all security policies to cover all forms of data over all forms of transmission. However, the policy cannot remain fixed – encryption routines may be found to be ineffective and newer techniques adopted. The best encryption techniques are those that are made available to public scrutiny, withstand rigorous testing, and are based on accepted standards and protocols [7].

4.1 Security Standards for Data Transmission

The workgroup adopted the following standards for the transmission of telehealth data:

- **4.1.1 All telehealth applications will meet all existing legal standards for secure data transmission, including federal, state and local standards.**

The workgroup recognizes that security standards do not apply to the transmission of all forms of telehealth data. The transmission of "live video" data, as occurs during videoteleconferencing, typically is not secured (perhaps to constraints on timing and volume of packet sizes). "Live audio" data (e.g. voice or stethoscope) is also typically not

secured. Note that securing live audio data would then suggest that telephone calls between consulting physicians must also be secured. For these reasons, the following standards for security only apply to "non live-video/audio" data at this time (pending changes in technologies).

- **4.1.2 All systems transmitting data outside an organization's LAN or over POTS or WAN connections, will encrypt the data to maintain privacy, will provide a means for maintaining validating data integrity, and will provide a means for authenticating the source of the data at the user level.**

- **4.1.3 The acceptable procedures and algorithms for providing security are those outlined in the "HCFA Internet Security Policy" and the "Health Insurance Portability and Accountability Act of 1996", or subsequent upgrades to these regulations.**

- **4.1.4 VPN (Virtual Private Network) hardware and software will conform to IETF standards (e.g. IPSec, IPv6) [8] and not employ techniques that are proprietary to a manufacturer. Vendors employing VPN solutions will demonstrate the true throughput of such systems and indicate any performance degradation resulting from their implementation due to CPU utilization.**

Recognizing that security standards are evolving and moving towards more restrictive measures, the workgroup believes in the immediate adoption of more restrictive standards than currently implemented by HCFA. The Technical workgroup expects Federal standards to change, as proposed changes are currently in circulation. The new standards are clearly on the horizon and, recognizing that software has a finite lifetime, it is better to guarantee the software is useful in the future. Software that fails to meet these standards may require expensive upgrades or outright replacement in the near future. Consequently, telehealth applications should meet the current HCFA standards for the transmission of all telehealth data outside a local area network, regardless of the use of the Internet or whether or not the data is HCFA data. In addition, while HCFA does not specify hash function or other measures to ensure data integrity, the Technical workgroup believes a standard should be set to establish a minimum procedure for ensuring data integrity.

Consequently, the standard calls for secure transmission of data anywhere outside the LAN supported by an organization. Data transmission over POTS or WAN connections must be secure. Furthermore, the only acceptable techniques are those detailed by HCFA and HIPAA. Both HCFA and HIPAA specifications call for open standards for encryption algorithms, whereas software such as First Class server uses a proprietary algorithm that is not publicly available. There was considerable discussion over the value, or danger, in using an algorithm that has not been held up for public scrutiny [9]. One solution, for First Class and other email-based systems, is to use client-side security to provide S/MIME or other encryption techniques rather than relying on the proprietary server-side techniques.

VPN systems using open standards are more likely to work with hardware from various manufacturers. However, users of a VPN-based system should be aware that IPSec cannot authenticate individual users and may use the 56-bit DES protocol that may eventually not meet Federal standards. VPN solutions that employ the more secure Triple-DES solution (168 bit encryption) have been know to demand significant CPU utilization such that performance of other software suffers significantly and true network throughput (bit rate) over the VPN may drop as much as 80% [10]. In such cases, a separate crypto accelerator may significantly improve overall performance. Vendors must demonstrate the effect of any VPN solution on system performance and network throughput.

It should be noted that the National Institute for Standards and Technology (NIST) has developed four levels of security standards which apply to "unclassified information within computer and telecommunication systems (including voice systems)" [11]. The "Federal Information Processing Standards' (FIPS) allow manufacturers to apply for certification at increasingly more secure levels. Manufacturers whose equipment meets or exceeds "Security Level 3" may meet all proposed HIPAA standards for all forms of data communication, including audio and video.

4.2 Security Standards for Data Storage

The workgroup adopted the following standard for the storage of telehealth data:

- **4.2.1 All telehealth applications will minimize the quantity of data stored outside secure server databases.**

This provides the greatest capability to secure and archive patient data. Client-server software applications are the best example of this technique. Databases located on secure servers will employ proper backup and archive operations. It is recommended that existing IS or HIS staff be involved in these procedures, as they are already cognizant of such procedures for other patient data.

4.3 Security Standards for Access to Data

The workgroup adopted the following standard for accessing telehealth data:

- **4.3.1 Administrative controls will be implemented by each health care organization to restrict access to telehealth data to "credentialed user", including restricting the senders and recipients of such data. Telehealth software will support this capability.**

Clearly, health organizations need to maintain access control to the telehealth data by implementing policies for determining who can (and cannot) access the multimedia telehealth data. Moreover, the organization must also be able to limit the movement of this data, by limiting the capability of users to send and receive data from other users and organizations. Telehealth software must provide this administrative capability.

This capability may have the negative effect of restricting the use of telemedicine when it is absolutely needed. A late-night consult requiring an urgent transmittal of data to a "non-credentialed user" will require administrative access to the system security. It is anticipated that vendors will desire to provide remote administration tools to facilitate this procedure. Alternatively, an organization may choose to disable this feature and not prevent any valid users from sending data outside the system. However, such a decision should be a choice for the organization to make (i.e. the software should support enabling/disabling this feature), and should not be forced on an organization by a limitation in the software design (i.e. the feature is not present).

5.0 File Formats

The workgroup failed to reach a consensus on specific file formats that must be adopted by telehealth projects, to promote interoperability and to provide a path for future access to the file structures. The following key points were raised in regards to file formats:

- The workgroup unanimously accepts the concept of "open file formats". This issue is critical to the ability to access patient data in future years, beyond the lifetime of the software. This issue is also critical to the interchange of data across systems.

- It is difficult to discuss "open" versus "closed" (or proprietary) standards when discussing file formats, because many manufacturer-specific formats have become *defacto* standards in recent years. Examples includes Microsoft Word files for text documents, CompuServe GIF files for images, Apple QuickTime for video, and Adobe PDF files for complex documents. Moreover, the wide range of data types (e.g. text, still image, movie, sounds, temporal data) results in a wide range of file formats from many manufacturers.

- "Open standards" typically refers to industry-wide standards or standards approved by manufacturer-neutral organizations whereas "closed standards" typically refers to proprietary formats. Where a clear open standard exists, that file format should clearly be endorsed. The MPEG standard, issued by the Moving Picture Experts Group, is one example of a file format that is clearly acceptable and is not manufacturer specific. Others include JPEG, JPEG 2000, HL7 and DICOM. Manufacturer-specific file formats that have become *defacto* standards include TIFF, GIF, Bitmap, HPGL, PIC, PCL, PostScript, WMF, and PICT. Some image file formats permit the user to specify "proprietary tags" (e.g. JPEG) and compressions, which effectively prohibits other code from reading the file format.

- Consequently, the Work Group did not reach a clear consensus on what file formats are acceptable. It was also recognized that, in some instances, no "open standard" currently exists (temporal EKG or EEG data, for example). In those cases, the file format is specific to the equipment manufacturer and the work group may not be able to set standards.

The following standards were adopted by the workgroup:

- **5.0.1 Telehealth systems will provide the capability for storing or exporting data to an appropriate "industry standard" or "open standard" file format, when such a format exists.**

- **5.0.2 Systems that only provide the capability for storing data in a "proprietary" or "manufacturer-specific" file formats are only acceptable when no other reasonable alternative exists. In such a case, the manufacturer will provide a complete file specification, including details on the bit-level format of the file and underlying algorithms inherent to the data stored in the file.**

- **5.0.3 Compression algorithms and levels of compression for digital images will be appropriate to the clinical use of the image. Clinical trials will be used to demonstrate the compressed images satisfy the diagnostic needs of the clinicians.**

- **5.0.4 Telehealth systems are encouraged to adopt ANSI standard file formats, such as HL7 and the XML variant of HL7, for the transmission of character-based data.**

The workgroup recognizes that the majority of telehealth data consists of electronic images, and a wealth of image file formats exist. A significant problem arises when manufacturers develop powerful compression algorithms (e.g. proprietary wavelet techniques) to reduce the size of the image file, but cannot publish the techniques or the final file format. In these cases, future access to the images depends on the software from the manufacturer; access to these images will fail when the software product fails to work. The problem is removed if the manufacturer provides the capability to export the images to a standard file format (and a potentially much larger file size) which may be viewed by other software.

In those cases where the manufacturer utilizes a "lossy" compression algorithm to reduce file size, the vendor must demonstrate through clinical trials that the resultant image provides diagnostic quality images for the end user.

Some data has no "well accepted" standard file format. Examples include EEG and EKG data. In this case, the above standards require manufacturers to provide a complete specification of the file format to ensure future compatibility with other software products, or at least the ability to write programs to access the internal data in the file.

The workgroup agrees that a standard should be determined regarding the file format for transmitting data between systems. These file formats may be considered "metafile" formats or "complex" file formats. For character-based data (i.e. text rather than binary data), an emerging international standard is the HL7 file format [12]. HL7 is becoming a standard for interchanging data between telehealth systems. Another exciting prospect is the emerging support for an XML (eXtensible Markup Language) variant of HL7, expected to be supported in the upcoming HL7 v3.0 specification [12]. XML v1.0 is a subset of SGML (Standard Generalized Markup Language) that has been endorsed by the World Wide Web Consortium [13].

It is reasonable to expect HL7 and XML to have finite lifetimes as international standards for data exchange. This is one example of the caveat expressed earlier in this document, that technical standards are only viable for a finite length of time and this document must undergo change with time.

6.0 Software

The workgroup reviewed issues critical to the software design of a telehealth system. Software issues mostly focused on components that affect security , and operating systems. The workgroup did not feel it was appropriate to restrict telehealth systems to a specific platform or technology. The following issues were raised:

- Security policies at the U.S. Air Force bases are generally the most restrictive of all partners in the Alaska Federal Health Care Partnership. Generally, Air Force rules are stricter than Department of Defense rules.
- Software using ActiveX technologies is generally "not allowed" in Air Force software due to security concerns, and Java is to be avoided. A waiver can be obtained in some cases to relax these rules.
- Microsoft operating systems dominate the market as expected. Windows 2000 is not projected to be an operating system at Air Force bases for about 18 months – it is currently considered "too new". Air Force requires Windows NT v4.0. ANMC has a similar policy, and Bartlett Hospital is migrating to this also. Questions remain about driver support for Windows NT (e.g. USB, biometric devices), but drivers seem to becoming available.
- Email at Air Force is restricted to 2 Meg limit. FTP is better option for larger file transfer. Air Force can accept encrypted email, but must be able to get at the header of the email.
- A web-based interface is better for the Air Force – only have to open port 80 and it is easier to pass traffic. Software must be capable of working through a proxy server. SSL is allowed at Air Force.

The following standards were accepted:

- **6.0.1 All potentially harmful software components (e.g. ActiveX and JAVA controls) in the software will be licensed controls.**

- **6.0.2 Telehealth vendors will be aware of security concerns and restrictions placed on the transport of data when promoting telehealth solutions in Alaska.**

Telehealth, especially in Alaska, often crosses political boundaries and involves parties from a variety of organizations. The examples obtained by the workgroup indicate that security concerns at the Air Force bases would prohibit those sites from adopting software solutions that may be acceptable to other organizations. A systems that was acceptable to all sites may still fail to work due to limitations imposed by the Air Force on file sizes passing through their email system. A telehealth vendor must be responsible and not promote a product when the product may fail to work, or fail to be accepted, in the various technical environments.

7.0 Videoconferencing

Videoconferencing (VtC) is a dominant vehicle for providing telehealth solutions, especially over wide bandwidth connections that are becoming more available in Alaska. The workgroup felt that interoperability is becoming less of an issue between VtC units as more manufacturers adhere to standards set by the International Telecommunications Union [14]. The dominant standards that apply to current technology are:

- ITU-T H.320 for circuit switched [15]
- ITU-T H.323 for packet switched [16]
- ITU-T H.324 for POTS bandwidth [17]

The following standard was adopted by the workgroup:

- **7.0.1 All videoconferencing equipment deployed for telehealth systems will satisfy the appropriate H.3xx standard for the transmission technology used to connect to remote sites.**

Satisfying the ITU-T standards promotes interoperability, but does not guarantee successfully connectivity or end user satisfaction. A significant issue that must be faced by any telehealth system that relies on videoconferencing is the limited bandwidth, satellite delays, and poor connectivity that often exist between remote locations. The above ITU-T standards may be "tweaked" for improved performance over such poor connections. For example, Alaska is the only environment on earth where AT&T uses satellite connectivity for voice signals, but local corporations use H.323 teamstations from Intel that are tweaked to satellite communication. Such technical improvements may still not be capable of producing a "clinically acceptable" videoconferencing system. Consequently, the following standard was adopted:

- **7.0.2 Telehealth systems will involve clinicians throughout the design and testing phase of a videoconferencing system over the expected connectivity to assure clinical acceptance of the system.**

Multicasting, the process of broadcasting live video to more than one end user, will become a target of telehealth systems especially for delivering distance education. In these cases, caching video locally within an organization can improve performance and provide later replay of the video. Multicasting often requires a different client software program, which may be proprietary and costly for bulk licenses. The following standards were adopted for multicasting and caching of videoconferencing systems:

- **7.0.3 Organizations should be encouraged to cache video data locally, to improve performance.**

- **7.0.4 Multicasting client software will be nonproprietary and free.**

8.0 Support and Maintenance

Telemedicine systems are expected to have 24 hour per day, 7 day per week uptime and access. However, because a telemedicine system is composed of many disparate parts connecting remote providers, the integrity of the entire system may not be under the control of a single vendor. Typically, a vendor that supplies the software and possibly the hardware has no control over the reliability of the network connection (WAN or POTS). It is reasonable to set expectations on the reliability of the vendor-supplied components and to expect support and minimum levels of quality of service.

The following standards were adopted by the workgroup:

- **8.0.1 Telemedicine systems will be expected to meet 24 hour per day/7 day per week uptime and access for users. Vendors will identify their capability and/or limitations of reaching this goal by identifying those portions of the system within their scope and, within this scope, identify anticipated uptime.**

- **8.0.2 Vendors will identify all support mechanisms (e.g. 24 hour telephone support) to attain maximal uptime of the telemedicine system, and identify all time constraints that may reduce the uptime. This includes identifying delays in providing consumables, turnaround time on repairs, and time to provide replacement parts where applicable.**

- **8.0.3 Vendors will identify all potential future costs to the customer, including costs for continued licensing fees, warranty costs, consumables, support options, anticipated recurring costs, upgrade options, and maintenance fees. Vendors will also identify expected lifetime and replacement costs for all hardware components.**

The workgroup also encourages potential customers to aggressively examine the capability of a vendor to provide a *sustainable* telehealth solution. Recognizing that selecting a telemedicine vendor is both a "business" and a "technical decision", this decision should be made by reviewing the long-term viability of the vendor. In addition to the business criteria that would be used to select a vendor (including corporate history), customers should consider the technical history of the product being marketed by the vendor.

The following standard was adopted by the workgroup:

- **8.0.4 Vendors will provide customers with information describing the current installed customer base for the telemedicine product, a technical history including planned and actual release dates of product releases / upgrades / features, future product plans and planned release dates, reports of currently identified problems and unresolved issues, and a description of the product's technical quality assurance and testing procedures.**

9.0 Telecommunications

Telehealth vendors often claim to be able to provide telehealth solutions in Alaska, without specific knowledge about telecommunications systems in Alaska. The telecommunications structure in Alaska is constantly evolving, and represents the highest and lowest technology systems available. Vendor assumptions about the availability of high speed connectivity ("just get an ISDN line") and land-based lines (rather than satellite connectivity) are fairly common. Even modem-based solutions have proven to be ineffective over poor POTS connections that suffer from high noise, low bandwidth, and dropped connections.

The following standard was adopted by the workgroup:

- **9.0.1 Vendors offering telemedicine systems will be familiar with the telecommunications systems in Alaska, and demonstrate the efficacy of using their solutions *in situ*.**

10.0 References

[1] State of Alaska, Department of Health & Social Services, "Alaska Telehealth Advisory Commission: Final Report," June 1999 (http://www.hss.state.ak.us/atac/).

[2] Federal Standard 1037C, "Telecommunications: Glossary of Telecommunication terms," (http://www.its.bldrdoc.gov/fs-1037/)

[3] National Research Council, *For the Record. Protecting Electronic Health Information*, Washington: National Academy Press, 1997.

[4] Federal Privacy Act of 1974, 5 U.S.C. § 552a (1994 & Supp. II 1996) (amended 1997, 5 U.S.C.A. § 552a) became effective on September 27, 1975 (http://www.usdoj.gov/04foia/04_7_1.html).

[5] HCFA Internet Security Policy (http://www.hcfa.gov/security/isecplcy.htm).

[6] Security and Electronic Signature Standards (http://aspe.os.dhhs.gov/admnsimp/nprm/seclist.htm) .

[7] B. Schneier, *Applied Cryptography 2nd Ed.*, New York: John Wiley & Sons, 1996.

[8] Internet Engineering Task Force (http://www.ietf.org) .

[9] B. Schneier, *E-Mail Security*, New York: John Wiley & Sons, 1995.

[10] A. Croll and B. Rothke, "Crypto Accelerators: Fast … & Secure," Information Security, Jan 2000 (http://www.infosecuritymag.com/jan2000/cover.htm).

[11] Federal Information Processing Standards Publication 140-1 (http://www.itl.nist.gov/fipspubs/fip140-1.htm).

[12] Health Level 7 (http://www.hl7.org/).

[13] World Wide Web Consortium: XML home page (http://www.w3.org/XML).

[14] International Telecommunications Union (http://www.itu.int/ITU-T/index.html).

[15] International Telecommunications Union: Recommendation H.323 (02/98) - Packet-based multimedia communications systems (http://www.itu.int/itudoc/itu-t/rec/h/h320.html).

[16] International Telecommunications Union: Recommendation H.323 (02/98) - Packet-based multimedia communications systems (http://www.itu.int/itudoc/itu-t/rec/h/h323.html).

[17] International Telecommunications Union: Recommendation H.324 (02/98) - Terminal for low bit-rate multimedia communication (http://www.itu.int/itudoc/itu-t/rec/h/h324.html).